



(12) Translation of
European patent specification

(11) NO/EP 2879008 B1

NORWAY

(19) NO
(51) Int Cl.
G05B 9/02 (2006.01)
B61L 19/06 (2006.01)
B61L 21/04 (2006.01)

Norwegian Industrial Property Office

(21)	Translation Published	2018.11.12
(80)	Date of The European Patent Office Publication of the Granted Patent	2018.07.04
(86)	European Application Nr.	13194789.7
(86)	European Filing Date	2013.11.28
(87)	The European Application's Publication Date	2015.06.03
(84)	Designated Contracting States:	AL ; AT ; BE ; BG ; CH ; CY ; CZ ; DE ; DK ; EE ; ES ; FI ; FR ; GB ; GR ; HR ; HU ; IE ; IS ; IT ; LI ; LT ; LU ; LV ; MC ; MK ; MT ; NL ; NO ; PL ; PT ; RO ; RS ; SE ; SI ; SK ; SM ; TR
(73)	Proprietor	Thales Management & Services Deutschland GmbH, Thalesplatz 1, 71254 Ditzingen, Tyskland
(72)	Inventor	Müller, Frank, Hämmerlingstrasse 15, 12555 Berlin, Tyskland
(74)	Agent or Attorney	TANDBERG INNOVATION AS, Postboks 1570 Vika, 0118 OSLO, Norge

(54)	Title	Method for handling a safety critical command in a computer network
(56)	References Cited:	DE-A1- 4 432 419, EP-A1- 2 253 524, DE-A1-102006 029 851, DE-A1-102010 015 285, DE-A1-102005 013 194

Enclosed is a translation of the patent claims in Norwegian. Please note that as per the Norwegian Patents Acts, section 66i the patent will receive protection in Norway only as far as there is agreement between the translation and the language of the application/patent granted at the EPO. In matters concerning the validity of the patent, language of the application/patent granted at the EPO will be used as the basis for the decision. The patent documents published by the EPO are available through Espacenet (<http://worldwide.espacenet.com>) or via the search engine on our website here: <https://search.patentstyret.no/>

Patentkrav

1. Fremgangsmåte for å håndtere en sikkerhetskritisk kommando ($f_i(e_k)$) i et datanettverk med en sikker datamaskin og en ikke sikker operatørterminal, hvor kommandoen vedrører en transaksjon på et element (e_k), hvor fremgangsmåten omfatter:

- overføring av kommandoen ($f_i(e_k)$) fra den ikke sikre operatørterminalen til den sikre datamaskinen;

- generering av en TAN(T), hvor TAN(T) identifiserer kommandoen; hvor fremgangsmåten videre er karakterisert ved

- generering av en første kjørbare kode (A) og en andre kjørbare kode (B) ved den sikre datamaskinen, hvor den andre koden (B) inneholder TAN(T), og den første koden (A) er i stand til å vise en spørring på en fremvisningsanordning ved den ikke sikre operatørterminalen og den andre koden (B) er i stand til å muliggjøre gjennomføring av transaksjonen;

- kryptering av kodene (A, B) ved den sikre datamaskinen;

- overføring av de krypterte kodene (A, B) til den ikke sikre operatørterminalen;

- dekryptering av kodene (A, B) ved den ikke sikre operatørterminalen;

- kjøring av den første koden (A) på den ikke sikre operatørterminalen, hvorved en spørring vises for operatøren med en anmodning om å bekrefte om den kritiske kommandoen skal utføres eller avbrytes;

- ved bekreftelse av operatøren, kjøring av den andre koden (B) og overføring av TAN(T) til den sikre datamaskinen.

2. Fremgangsmåte ifølge krav 1, karakterisert ved at ved kjøring av den første koden (A), et vindu vises på fremvisningsanordningen, hvor vinduet viser en gjenspeiling av kommandoen og minst to knapper for henholdsvis bekreftelse og avbrytelse av transaksjonen.

3. Fremgangsmåte ifølge krav 2, karakterisert ved at vinduet videre viser informasjon om status (s) for elementet (e_k) og eller status for omgivelsene til

elementet (e_k) som transaksjonen skal utføres på.

4. Fremgangsmåte ifølge ett av de foregående krav, karakterisert ved at den andre koden (B) inneholder en tilbakekallsfunksjon for den første koden (A), hvor
5 tilbakekallsfunksjonen overfører TAN(T).
5. Fremgangsmåte ifølge ett av de foregående krav, karakterisert ved at TAN(T) er utstyrt med en tidsbegrensning.
- 10 6. Fremgangsmåte ifølge ett av kravene 1 til 5, karakterisert ved at den første koden (A) og den andre koden (B) er innlemmet i én programfil.
7. Fremgangsmåte ifølge kravene 1 til 5, karakterisert ved at den første koden (A) og den andre koden (B) er separate programfiler.
15
8. Fremgangsmåte ifølge ett av de foregående krav, karakterisert ved at bekreftelsen fra operatøren utføres ved hjelp av en ettklikksteknikk.
9. Fremgangsmåte ifølge ett av de foregående krav, karakterisert ved at
20 fremgangsmåten anvendes for transaksjoner vedrørende skinnetransport eller andre ledede kjøretøy.
10. Bruk av et datanettverkssystem som omfatter midler tilpasset for å utføre fremgangsmåten ifølge ett av de foregående krav.
25
11. Bruk ifølge krav 10, karakterisert ved at en sikker datamaskin og en ikke sikker operatørterminal for sikre driftsprosesser på et forbestemt sikkerhetsintegritetsnivå, spesielt for jernbanetransport, er tilveiebragt, hvor den sikre datamaskinen og den ikke sikre operatørterminalen er forbundet med hverandre for å overføre meldinger, hvor
30 den ikke sikre operatørterminalen omfatter en fremvisningsanordning og er satt opp

for å identifisere en kryptert kode (A, B), for å dekryptere den krypterte koden (A, B)
og for å vise en spørring på fremvisningsanordningen,

 hvor den sikre datamaskinen er i samsvar med den forbestemte
sikkerhetskategorien og den ikke sikre operatørterminalen ikke er i samsvar med den

5 forbestemte sikkerhetskategorien.